UNIVERSITÀ DI PARMA
Dipartimento di Ingegneria e Architettura

Network vulnerabilities

Luca Veltri

(mail.to: luca.veltri@unipr.it)

Course of Cybersecurity, 2022/2023

http://www.tlc.unipr.it/veltri

Network Attacks

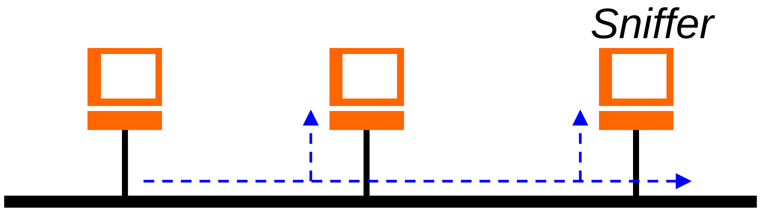
- There are different typologies of attacks that can occur in a networked scenario
- Generally, objectives of an attack include:
  - **impersonification of an entity**
    - violation of peer entity authenticity and/or data
  - **fraudulent gathering of personal data**
    - violation of confidentiality (and sometimes peer entity authenticity)
  - **damaging or denying of a service**
    - violation of availability

Network Attacks (cont.)

- Attack techniques include:
  - **data interception**
    - network eavesdropping (sniffing)
    - spoofing
    - redirection and routing attacks
  - **violation of authentication (and encryption) systems**
    - password cracking, guessing
  - **denial of service (against a network service or resource)**
    - e.g. via distributed attack
      - network flooding, distributed denial of service (DDoS)
  - **network and vulnerabilities scanning**
  - **exploitation of vulnerabilities**
    - protocol vulnerabilities
    - software vulnerabilities
  - **running malware**

Network eavesdropping

- Network eavesdropping or network sniffing is an attack consisting of capturing packets from the network transmitted by others' nodes and reading the data content
  - **in search of sensitive information like passwords, session tokens, or any kind of confidential information**
- The attack could be done by using tools called network sniffers (or protocol analyzers)
  - **these tools collect packets on the network and, depending on the quality of the tool, analyze the collected data like protocol decoders or stream reassembling**
- Can work in passive mode
  - **packets are simply captured, copied, and passed at user level for further analysis**
  - **requires to be along the path or in a broadcasting domain**



LAN eavesdropping

- In case of a LAN, the attacker configures the network interface for working in promiscuous mode capturing all packets passing through the network interface
  - **LAN with hub**
    - the hub duplicates every frame to all interfaces (ports)
  - **switched LAN**
    - a switch by default only transmits a frame to the destination port
    - there are attacks that may
      - make the device to switch from partitioning to broadcasting mode (fail-open mode), e.g. MAC flooding
      - redirect the traffic from one port to another; then the system may acts like a router between the source and destination (Man-In-The-Middle attack), e.g. arp spoof attack
  - **wireless LAN**
    - sniffing is possible if no encryption is used or if a crack attack is performed against the WiFi key

Network sniffer

- Most common network sniffers (or protocol analyzer) are:
  - **WireShark**
    - GUI
  - **tcpdump (unix)**
    - command-line
- Windows sniffers usually are based on winpcap or npcap DLL libraries
- Unix sniffers usually are based on the tcpdump libpcap library
- Usually they require root/admin privileges

Network sniffer detection

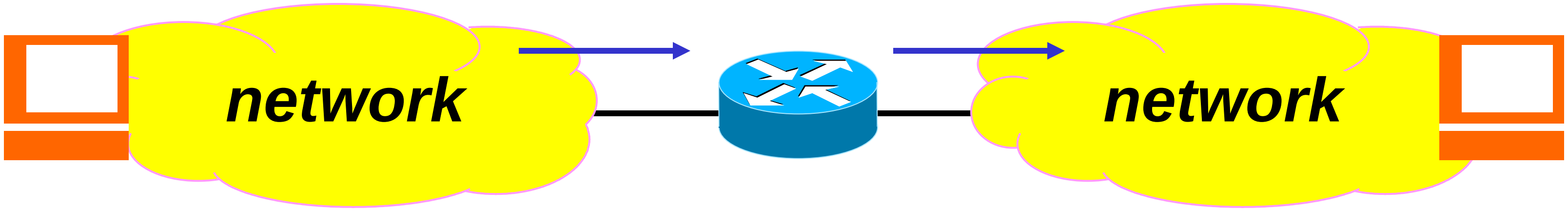
- The presence of a network sniffer may be detected by means of
  - **proper commands directly on the node used to run it, e.g.:**
    - ifconfig

```
eth0 Link encap:Ethernet HWaddr 00:10:4B:E2:F6:4C
          inet addr:192.168.1.8 Bcast:192.168.1.255 Mask:255.255.255.0
          UP BROADCAST RUNNING PROMISC MULTICAST MTU:1500 Metric:1
          RX packets:1016 errors:0 dropped:0 overruns:0 frame:0
          TX packets:209 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
```

    - cpm (Check Promiscuous Mode)
    - ifstatus
  - **specific sniffing detection tools that exploit unusual behaviours of the OS when working in promiscous mode**

Man-In-The-Middle attack (MITM)

- Using a network sniffer in a LAN is not the only mechanism for packet interception
- Packet interception can be also performed by means of
  - **intercepting packet in a node already along the path**
  - **exploiting vulnerabilities of routing and/or address resolution protocols**
    - e.g. ARP spoofing, ICMP redirect, DNS record poisoning, etc.
- In these cases, the attack is called Man-In-The-Middle (MITM)
  - **the attacker is also able to modify the packets**



Spoofing attack

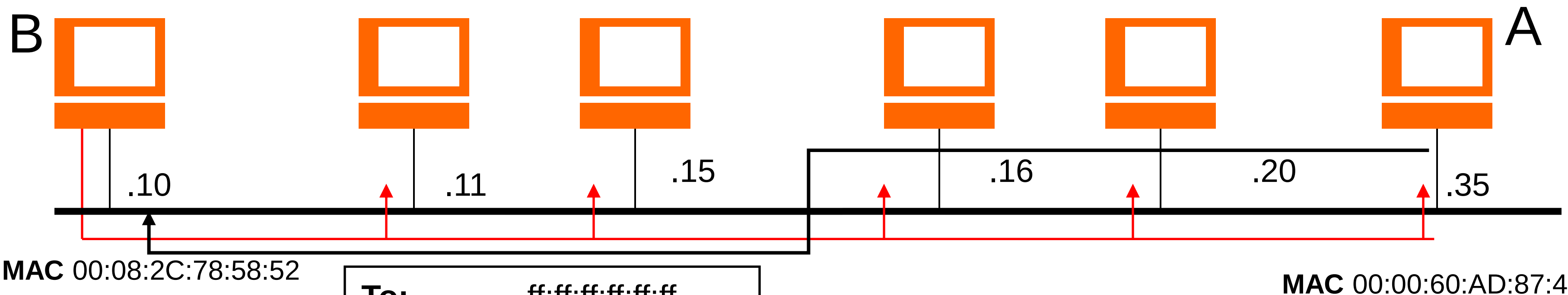
- A technique where one entity (attacker) successfully masquerades as another by falsifying data origin (spoofing)
- It could be performed at different layers
  - **Layer 2 (Link)**
    - MAC spoofing, ARP spoofing
  - **Layer 3 (IP)**
    - IP spoofing
  - **Layer 4 (Transport)**
    - UDP or TCP spoofing
  - **Layer 7 (Application layer)**
    - e-mail address spoofing
    - VoIP Caller ID spoofing
    - webpage spoofing (also known as phishing)
- When the fake identity (spoofed) is a real identity, it leads to social engineering attacks

ARP Spoofing

- An attacker sends fake ("spoofed") Address Resolution Protocol (ARP) messages onto a Local Area Network
  - **generally, the aim is to associate the attacker's MAC address with the IP address of another host (e.g. the default gateway), causing any traffic meant for that IP address to be sent to the attacker instead**
  - **also referred to as ARP poisoning**
  - **can only be used on networks that make use of the ARP protocol and is limited to local network segments**
- ARP spoofing allows an attacker to intercept data frames on a LAN, modify the traffic, or stop the traffic altogether
  - **often used as an opening for other attacks, such as man in the middle, session hijacking, or denial of service attacks**
- ARP spoofing may also be used as non-attacking technique
  - **E.g. by Captive Portals, or in Mobile IP**

Normal ARP protocol behaviour

Subnet 192.168.10.0/24



To:	ff:ff:ff:ff:ff:ff
From:	00:08:2C:78:58:52
MAC-T	00:00:00:00:00:00
MAC-S	00:08:2C:78:58:52
IP-T	192.168.10.35
IP-S	192.168.10.10

ARP request

Who-has 192.168.10.35 ?

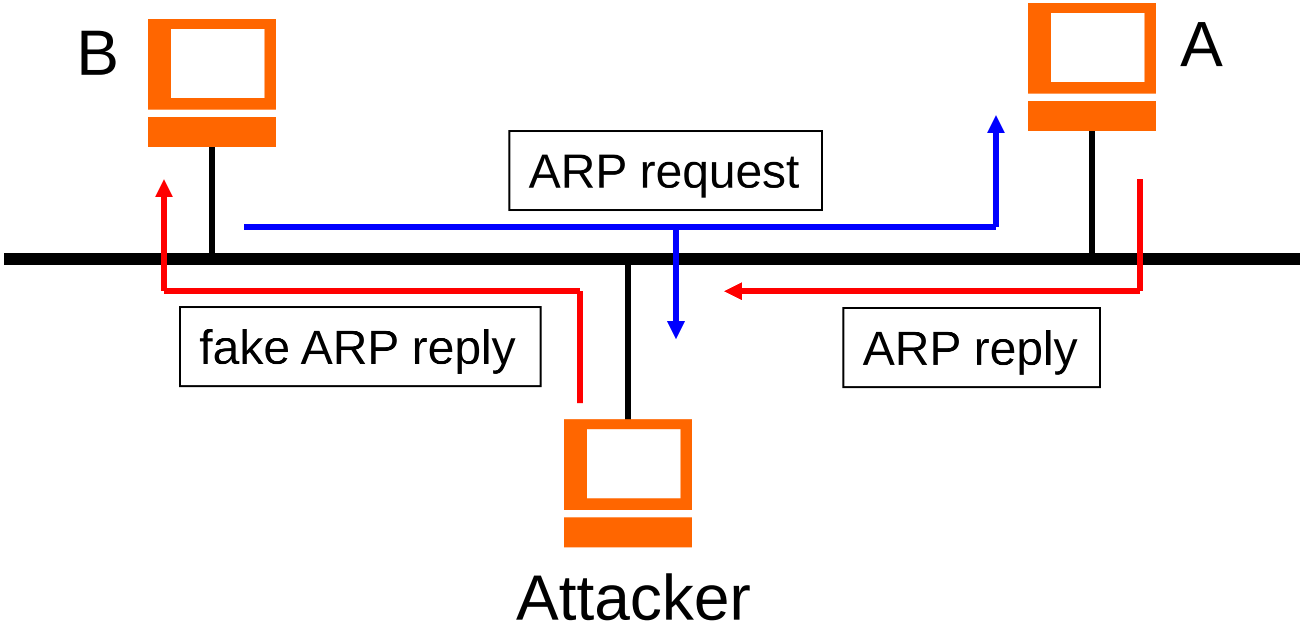
ARP reply

192.168.10.35 is-at 00:00:60:AD:87:44

To:	00:08:2C:78:58:52
From:	00:00:60:AD:87:44
MAC-S	00:00:60:AD:87:44
MAC-T	00:08:2C:78:58:52
IP-S	192.168.10.35
IP-T	192.168.10.10

- When receiving the replay, the client adds the pair {MAC_addr,IP_addr} to its ARP table

ARP Spoofing (cont.)



Defenses against ARP spoofing

- Static ARP entries
  - **IP-to-MAC mappings in the local ARP cache can be statically defined, and then hosts can be directed to ignore all ARP reply packets**
  - **however it results in a big effort for maintenance**
- ARP spoofing detection software
  - **it detects ARP spoofing based on cross-checking of ARP responses**
    - the existence of multiple IP addresses associated with a single MAC address may indicate an ARP spoof attack, although there are legitimate uses of such a configuration
  - **may be implemented in individual hosts or may be integrated into Ethernet switches or other network equipment**
- OS security
  - **operating systems may react differently**

MAC Spoofing - Port stealing

- Another type of MAC spoofing attack
- It floods the LAN with packets with a spoofed source MAC address
  - **e.g. by sending many layer-2 packet to its real MAC address**
  - **this process "steals" the switch port of the spoofed host**
  - **packets destined to "stolen" MAC addresses will be received by the attacker, winning the race condition with the real port owner**
  - **when the attacker receives packets for "stolen" hosts, it may stop the flooding process and performs an ARP request for the real destination of the packet**
  - **when it receives the ARP reply it's sure that the victim has "taken back" his port**
- This technique is useful to sniff in a switched environment when ARP poisoning is not effective (for example where static mapped ARPs are used)

IP Spoofing

- Creation of Internet Protocol (IP) packets with a forged source IP address
  - **most frequently used in MITM or denial-of-service attacks (DoS/DDoS)**
  - **also a method of attack used by network intruders to defeat network security measures, when trust relationships exist between machines based on IP addresses, e.g.:**
    - RPC services
    - X Window System
    - the R services suite (rlogin, rsh, etc.)
    - any service that uses IP address authentication
  - **sometimes used to by-pass firewalls (e.g. using the IP source routing option)**

TCP spoofing - TCP session hijacking

- Technique for establishing or intercepting a TCP session (connection) between two machines
- Two possibilities:
  - **source routing**
    - the initial hijacking method used involved using the source routing option of the IP protocol
    - this option made it possible to specify the path IP packets were to follow
    - The destination reverses the path in the opposite direction
  - **blind attack**
    - the only possible technique when source routing is disabled and the attacker is not in the same network of the two machines
    - involves sending packets as "blind attacks“
    - requires the establishment of a TCP connection (3-way handshake) without receiving responses, by trying to predict sequence numbers
    - more complex than an IP spoofing attack

TCP Spoofing (cont.)

- (Spoofed) TCP 3-way handshake

H	>	SYN	>	B	**start of connection setup**
A	<	SYN/ACK	<	B	**response of the victim, set to the spoofed host**
H	>	ACK	>	B	**handshake completed**
H	>	PSH	>	B	**data**

- TCP uses 32 bit Seq/Ack numbers
  - **these numbers make it relatively hard to spoof the source address because successful spoofing requires guessing the correct initial sequence number (ISN) which is generated by the server in a non-guessable way**
  - **it is commonly known that a 32 bit number can be brute forced in a couple of hours given a fast (gigabit) network connection**

Denial of Service (DoS)

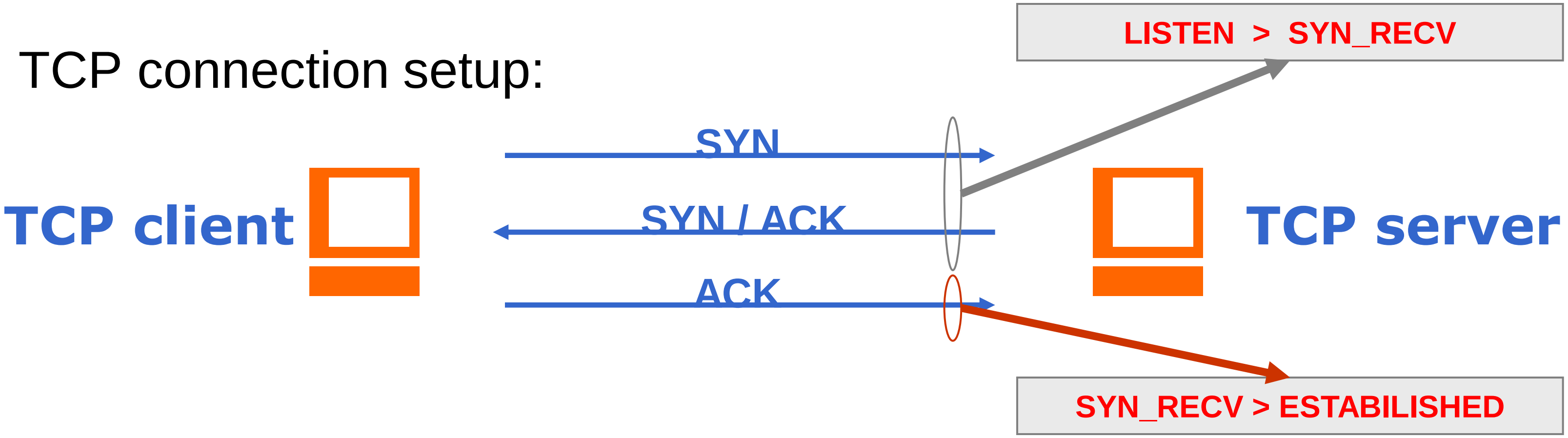
- Attack for making a machine or network resource unavailable to its intended users
  - **most common technique is flooding**
    - It consumemems victim resource (network bandwidth and/or processing capacity)
- Can be executed by
  - **a single node**
  - **two or more nodes**

DoS (cont.)

- The attack is successful in consuming resources on the victim by either:
  - **using a computer with greater computation power and/or large network bandwidth**
  - **taking advantage of a property of the victim system which enables an attack consuming vastly more of the victim's resources than the attacker's (an asymmetric attack)**
    - e.g. SYN flood
  - **using a large number of computers and directing them to attack as a group**
    - Distributed Denial of Service (DDoS) attack
    - a set (or network) of nodes controlled by a single entity
      - e.g. (ICMP) Smurf, botnet
- An attack may utilize a combination of these methods in order to magnify its power

DoS: SYN flood

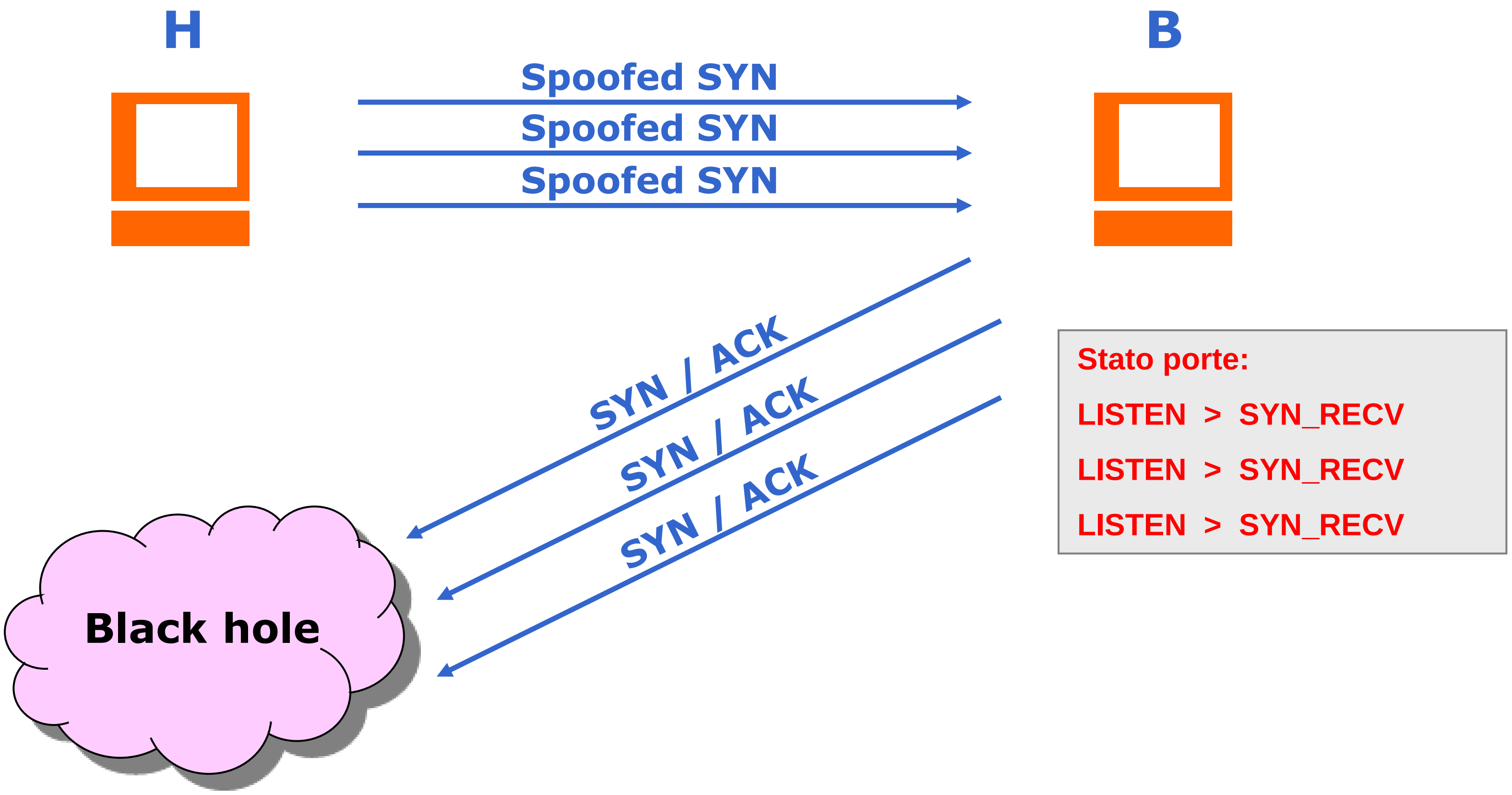
- TCP connection setup:



- TCP SYN flooding attack:
  - **A host sends a flood of TCP/SYN packets, often with a forged sender address**
    - each of these packets is handled like a connection request, causing the server to spawn a half-open connection, by sending back a TCP/SYN-ACK packet (Acknowledge), and waiting for a packet in response from the sender address (response to the ACK Packet)
    - however, because the sender address is forged, the response never comes
  - **These half-open connections saturate the number of available connections the server is able to make, keeping it from responding to legitimate requests until after the attack ends**

DoS: SYN flood (cont.)

- TCP SYN flooding attack:



H

B

Spoofed SYN

Spoofed SYN

Spoofed SYN

SYN / ACK

SYN / ACK

SYN / ACK

Black hole

Stato porte:

LISTEN > SYN_RECV

LISTEN > SYN_RECV

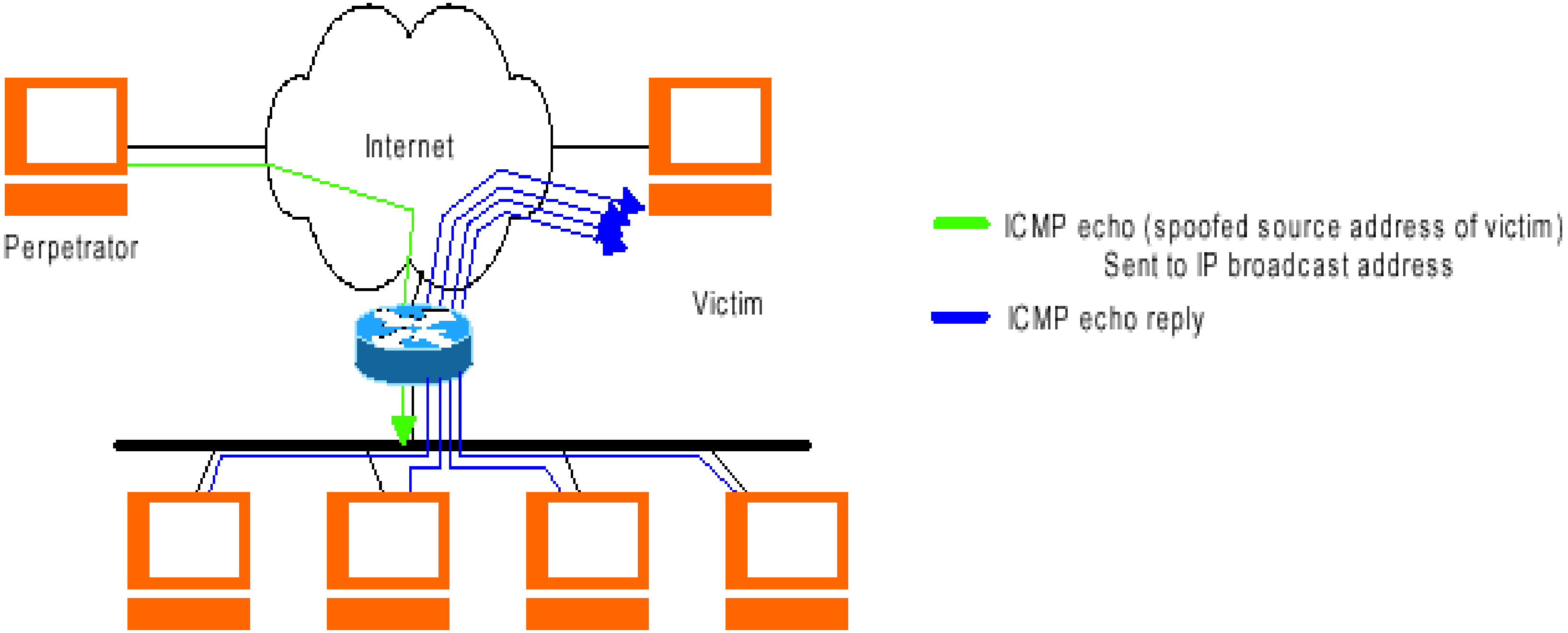
LISTEN > SYN_RECV

DDoS: Smurf

- A Smurf attack is a flooding DoS exploiting the possibility of sending packets to all computer hosts on a particular network via the broadcast address of the network
  - **the attacker sends large numbers of packets with the source address faked to appear to be the address of the victim**
  - **the network then serves as a smurf amplifier**
  - **the network's bandwidth is quickly used up, preventing legitimate packets from getting through to their destination**
  - **it relies on misconfigured network devices that allow the forwarding of broadcast packets**

DDoS: ICMP/Ping Flooding (Smurf)

- Ping flood is based on sending the victim an overwhelming number of ping packets


Internet
Perpetrator
Victim
ICMP echo (spoofed source address of victim)
Sent to IP broadcast address
ICMP echo reply

DoS Attack Defenses

- These attacks cannot be prevented entirely
- High traffic volumes may be legitimate
- Four lines of defense against DDoS attacks
  - **Attack prevention and preemption**
    - before attack
  - **Attack detection and filtering**
    - during the attack
  - **Attack source traceback and identification**
    - during and after the attack
  - **Attack reaction**
    - after the attack

Routing attacks

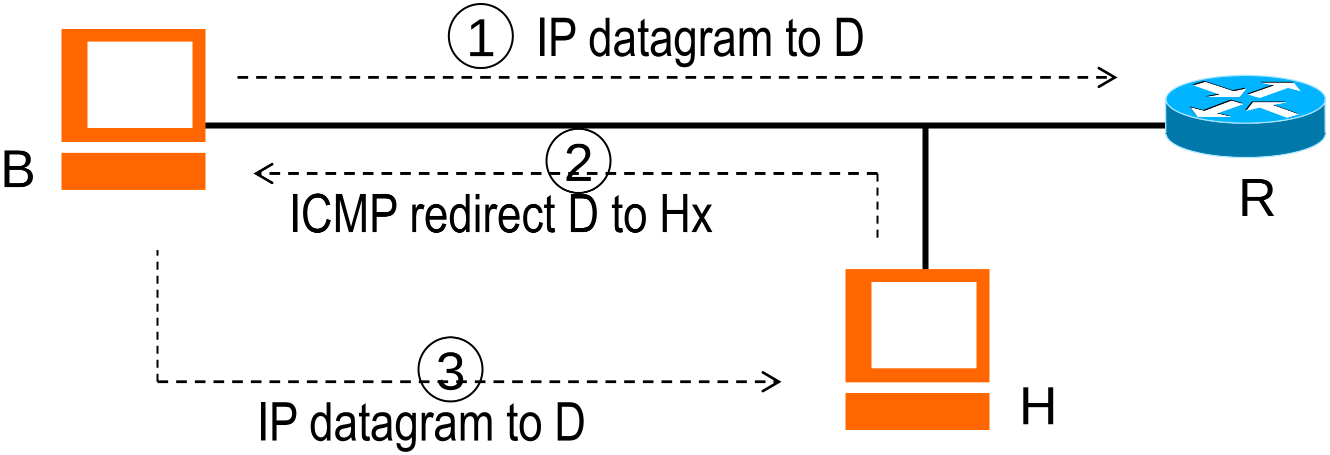
- Attacks that use vulnerabilities of dynamic configuration or routing mechanisms in order to redirect or block network traffic
- They may exploit:
  - **address resolution mechanisms (e.g. ARP or DNS)**
  - **Dynamic configuration protocols (BOOTP/DHCP)**
  - **routing protocols**
- They may operate at different protocol stack level:
  - **Layer 2 (Link)**
    - e.g. ARP spoofing, port stealing
  - **Layer 3 (IP)**
    - exploting ICMP or IGMP control protocols, dynamic host configuration protocols (BOOTP/DHCP/MobileIP), routing protocol (RIP and OSPF)
  - **Layer 7 (application)**
    - e.g. DNS poisoning

Routing attacks: ICMP Destination unreachable

- The attacker sends a spoofed *ICMP Destination unreachable* message to the victim in the same LAN
- Possible subtypes of *Destination unreachable*:
  - **Network unreachable**
  - **Host unreachable**
  - **Protocol unreachable**
  - **Port unreachable**
  - **Fragmentation needed but don’t fragment bit set**
  - **Destination host unknown**
  - **Destination network unknown**
- Can be used to mount a DoS attack
  - **e.g. in order to start a spoofing attack**

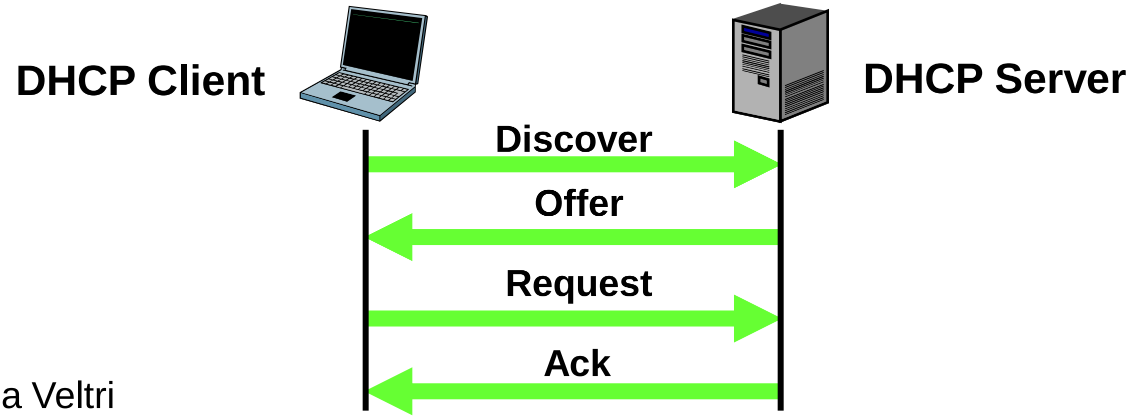
Routing attacks: ICMP Redirect

- The attacker sends a spoofed *ICMP Redirect* message to the the victim in the same LAN pretending to be a better route for a destination
  - **alternative respect to ARP spoofing**
  - **it uses standard ICMP message**
  - **all packets or connections to internet will be redirected to the new node which, in turn, may**
    - drop them (DoS)
    - forward them to the real gateway (MITM)



Routing attacks: BOOTP/DHCP attack

- Spoofing attack that exploits BOOTP/DHCP configuration protocols
- The attack pretends to be a DHCP server and tries to win the race condition with the real one to force the client to accept the attacker's reply
- This way the attacker is able to manipulate the IP, DNS or router parameters and hijack all the outgoing traffic generated by the DHCP clients
- The resulting attack is a half-duplex MITM or DoS attack



Application protocol attacks

- Exploiting specific application protocols (DNS, Mail, FTP, etc.)
- Examples:
  - **email**
    - mail spamming
    - mail spoofing
    - mail phishing
  - **DNS**
    - pharming – an attack aiming to redirect a website's traffic to another, bogus website
      - "hosts" file poisoning
        - changing the “`hosts`” file on a victim’s computer
      - DNS spoofing
        - returning a fake DNS record (either against a host or a DNS server)
      - DNS cache poisoning
        - exploitation of a flaw in the DNS software that can make it accept incorrect information

Vulnerability scanning

Vulnerability scanning

- Types of vulnerability scanners
  - **network and port scanner**
    - tells which hosts and network services are running and reachable
      - e.g. Nmap
  - **network vulnerability scanner**
    - looks for possible vulnerabilities associated to detected running application
      - e.g. Nessus, SAINT, OpenVAS
  - **web application security scanner**
    - automated crawling and testing of web applications
      - e.g. Indusface WAS, ScanMyServer, SUCURI, SSL Labs, Quttera, Detectify, Siteguarding, etc
      - https://owasp.org/www-community/Vulnerability_Scanning_Tools
  - **database security scanner**
  - **host based vulnerability scanner**
  - **single vulnerability test**

Network scanning

- Also refereed as network enumerating
- Activity through specific software for scanning a network for discovering active hosts and open ports (Port scanning)
  - **e.g. ping, traceroute, nmap**
- This is often used by administrators to check the security of their networks
- Can be used by hackers to identify running services on a host with the view to compromising it
- Related to network scanning are:
  - **Vulnerability scanning**
  - **Penetration test**

Network scanning (cont.)

- What a network scanner can do
  - **Host discovery**
    - identifying hosts on a network, for example listing the hosts which respond to pings, or which have a particular port open
  - **Port scanning**
    - enumerating the open ports on one or more target hosts
  - **Service version detection**
    - interrogating listening network services listening on remote devices to determine the application name and version number
  - **OS detection**
    - remotely determining the operating system and some hardware characteristics of network devices

Host Discovery

- Host discovery may be performed by using different techniques
  - **ICMP scan**
    - determines if a host responds to ICMP requests, such as echo (ping), netmask, etc
  - **TCP SYN/ACK/RST**
    - tries to open a TCP connection using port numbers
      - associtated to most common application services (e.g. HTTPd), or
      - by a given set
    - two modes (see later):
      - user space (TCP connect())
      - root space (TCP SYN/ACK/RST)

Host Discovery: ICMP Echo Request

- Host discovery through ICMP Echo Request (pingscan):
  - **ICMP echo datagrams are sent to a given host or to all hosts in a subnetwork**
  - **The attacker collects the replies and determines which hosts are actually alive**
- Example:

```
Starting nmap V. 2.12 by Fyodor (www.insecure.org/nmap/)
Host cisco-sales.ns.com (195.121.31.11) appears to be up.
Host sales1.ns.com (195.121.31.19) appears to be up.
Host sales4.ns.com (195.121.31.22) appears to be up.
Host sales2.ns.com (195.121.31.43) appears to be up.
Host sales3.ns.com (195.121.31.181) appears to be up.
Nmap run completed -- 256 IP addresses (5 hosts up) scanned in 1 second
```

Port scanning

- A port scanner may scan
  - **the most common port numbers, or**
  - **ports most commonly associated with vulnerable services, on a given host, or**
  - **a given list of TCP and UDP port numbers**
- The result of a scan on a target {host,proto,port} can be:
  - **Open or Accepted**
    - the host sent a reply indicating that a service is listening on the port
    - open ports may revel vulnerabilities associated with
      - the program responsible for delivering the service
      - the operating system that is running on the host
  - **Closed or Denied or Not Listening**
    - the host sent a reply indicating that connections will be denied to the port
  - **Filtered, Dropped or Blocked**
    - there was no reply from the host

Port scanning (cont.)

- Port scanning types:
  - **TCP scanning**
    - the simplest port scanners
    - use the operating system's network functions (e.g. connect() call)
    - if a port is open, the operating system completes the TCP three-way handshake, and the port scanner immediately closes the connection; otherwise an error code is returned
    - has the advantage that the user does not require special privileges
    - however, it prevents low-level control
  - **SYN scanning**
    - the port scanner generates raw IP packets itself (TCP SYN packet), and monitors for responses (TCP SYN-ACK packet), rather than use the operating system's network functions
    - the scanner responds with a TCP RST packet, closing the connection before the handshake is completed
    - also known as "half-open scanning", because it never actually opens a full TCP connection

Port scanning (cont.)

- Port scanning types: (cont.)
  - **ACK scanning**
    - it does not exactly determine whether the port is open or closed, but whether the port is filtered or unfiltered
  - **UDP scanning**
    - if a UDP packet is sent to a port that is not open, some systems respond with an ICMP port unreachable message
    - an alternative approach is to send application-specific UDP packets, hoping to generate an application layer response
- Note: there is debate over which scan is less intrusive on the target host between TCP connect or TCP SYN scans
  - SYN scan has the advantage that the individual services never actually receive a connection; however, the RST during the handshake can cause problems for some network stacks, in particular simple devices, like printers or other smart objects
  - connect scan uses more resources and may cause some services to crash

Network vulnerability scanners

- They usually combine a network scanner with a DB of known application weaknesses and vulnerabilities
  - **for each vulnerability they usually associate:**
    - degree of risk
    - recommendations on how to mitigate it

- Examples of vulnerability scanning tools:
  - **Nessus**
  - **OpenVAS**